Week 1

Computer Forensics Semester I 2024

Lecturer : Dr. Mbemba NDARA

Contact Information

- Lecturer: Dr. Mbemba Hydara
- E-mail: Hmbemba@utg.edu.gm
- /hydara777@gmail.com
- Cell Phone: 7369552

Course Objectives

By the end of this course, you should be able to:

- Explain reasons for Forensics policies and procedures
- Formulate policies and procedures
- Identify the steps in a forensics examination
- Conduct an Investigation
- Present the evidence in a court of law
- Scope from Crime scene to Trial

Learning Outcomes

At the end of the Course, you should be able to:

- Understand forensics concept and definitions
- What constitute a crime and identify categories of digital crime
- Understand Computer Forensics Investigation process
- Explain different types of evidence
- Analyse what affects admissibility of evidence
- Explain how electronic evidence differs from physical evidence
- Identify what computer forensics tools and techniques can reveal and recover
- Explain process of discovery and expert witness testimony

Course Outline

Weeks	Course Units/Topics	Lecturer
1	• Overview of Computer Forensics Course • Introduction to Computer Forensics	Dr. Hydara
2 - 3	• Admissibility of Electronic Evidence • Forensic Evidence and Crime Investigation • Computer Forensics and digital detective work	Dr. Hydara
3 - 4	• Role of evidence in solving physical and computer crime • Computer forensic Science • Computer and e-evidence process • Suppression, probable cause, and search warrants • Types of motives of cybercrimes • Computer Forensics investigators responsibility	Dr. Hydara
5-7	• E-evidence collection and Preservation • Tool, Environments, Equipment and Certification • Managing life-cycle of a case	Dr. Hydara
8-9	• Policies and Procedures • Forensics examination of computers and digital media	Dr. Hydara
10 -11	• Analysis, interpretation and documentation	Dr. Hydara
12 - 14	• Expert witness testimony	Dr. Hydara

Course Delivery Mode

- Lecture sessions
- Tutorials/Practical
- Group Presentation
- Directed Research
- Discussion tasks

Class Attendance

- Active participation of all students is encouraged in class
- Class sessions will involve interaction and discussions
- You are required to attend 80% of the entire semester session to avoid being reprimanded.
- The more effort you put into class session the better for the learning outcomes

Assessment Mode

- Attendance: minimum of 80% attendance is required
- Assessment: Formative and Summative
- Continuous Assessment (CA)
  Test = 20%
- Attendance: 5%
- = Term Assignment = 25 %
- Sub-Total = 50%
- Final Exams = 50%
- Overall Term score = 100%

Right of Others

- Respect your fellow students and keep cell phones in silence mode
- If you have to talk to someone kindly move outside.
- Distractions with mobile phones or Laptops will not be tolerated
- Active listening and participation is highly required

Special Assignment

- You will undertake a week research assignment/a case study during the semester
- You are required to complete all tests and assignment
- You will be notified when and how it will be carried out.

Late Submission of Work

- All assignments must be completed in accordance with given instructions.
- The assignment must be submitted in both soft and hard copy on or before submission date.
- It is your responsibility to make sure you submit your work on time.

Plagiarism

- We expects a high level of responsibility and academic honesty throughout the course.
- Plagiarism from the web, from portions of papers, and from any other source is an academic offense hence unacceptable.
- Be aware of the existence of a plagiarism software
- To avoid it, Simply acknowledge the work of others

Course Withdrawal

- University administration has set deadlines for withdrawal of any course for the Semester
- It is the student's responsibility to handle withdrawal requirements before closure of the portal
- Students will not be allowed to take exams only when they are not registered for the course.
- You must do the proper paperwork to ensure you are in compliance.

Make-Test/Exams

- No excuse will be accepted without prior written, or advance notice for absence.
- Should there be scheduling conflict, it is your responsibility to let the lecturer know well in advance

Reading Materials

- . R. Vacca, Computer forensics: Computer Crime Scene investigation, 2nd Ed. Hanover, NH, United States: Charles River Media, 2002.(ISBN No.: 978-1-58-450389-7).
- C. Altheide, H. Carvey, and R. Davidson, Digital Forensics with Open Source Tools: Using Open Source Platform Tools for Performing Computer Forensics on Target Systems: Windows, Mac, Linux, Unix, etc, 1st Ed. United States: Syngress Media,U.S., 2011.(ISBN No. : 978-1-59-749586-8).
- S. Bommisetty, R. Tamma, and H. Mahalik, Practical Mobile Forensics: Dive into Mobile Forensics on IOS, Android, windows, and blackBerry devices with this action-packed, practical guide. United Kingdom: Packt Publishing, 2014. (ISBN No. : 978-1783288311).
- G. Gogolin, Digital Forensics Explained, 1st Ed. Boca Raton, FL: CRC Taylor Francis, 2013. (ISBN No. : 978-1-43-987495-0)
- M. Dawson and M. Omar, Eds., New Threats and Countermeasures in Digital Crime and Cyber Terrorism. Boca Raton, FL, United States: Idea Group,U.S., 2015. (ISBN No.: 978- 1-46-668345-7)

Week 1

Introduction to Computer Forensics

Lecture Scope

Week 1

- Introduction to Computer Forensics
- Definitions
- Computer Forensics concepts
- Career opportunities

Scope contd.

- Industry opportunities
- Where Computer Forensics might be use
- Law & Investigations

Definitions

What is Computer Forensics?

Definition

Chapter 1

Forensics

- The process of using scientific knowledge in the collection, analysis, and presentation of evidence to the courts.
- Forensics means “to bring to the court.”

Computer Forensics

- The collection and analysis of data from computer systems, networks, communication streams (wireless) and storage media in a manner that is admissible in a court of law.

Definitions Contd.

- The process of uncovering and interpreting electronic data for use in a court of law.
- It involves the preservation, identification, extraction, and documentation of digital evidence.

Definitions

- Deals primarily with the recovery and analysis of latent evidence.
- Latent evidence such as fingerprints left on a window to DNA evidence recovered from blood stain

Importance of Digital Forensics

- Digital forensics helps in investigation of cybercrimes such as hacking, fraud, and data breaches.
- It helps in recovering lost or deleted data, and analysis of digital devices for evidence.

Key Concepts in Digital Forensics

Chain of Custody:

Maintaining the integrity of evidence by documenting its handling from collection to presentation in court.

Volatile data:

Data stored in temporary memory (RAM) that is lost when the system is powered off.

Digital Forensics Process

Identification:

Determine the scope of the investigation and the type of evidence involved.

Preservation:

- Ensure the integrity of evidence by making a forensic image.

Analysis:

- Examine the evidence using forensic tools and techniques

Presentation:

- Present findings in a clear and concise manner for use in legal proceedings

Industry Actors

- **Growing field :** Many becoming computer forensic specialists
  - Law enforcement
  - Private Security Companies
  - FBI, State and National Police,
  - Defense attorneys, judges and prosecutors
  - Independent Security Agencies
  - White hat or Ethical Hackers
- The evidence must be preserved and hold up in a court of law

Cybercrime

- Computer crime, cybercrime, information crime, and high-tech crime are all used interchangeably.
- Computer crime can be categorized into two areas:

Computer as target

- Computer or its data is the target of the crime

Cybercrime Contd.

Computer as Instrument

- Where computer is used to commit crime

Expert witness

- An is a qualified specialist who presents forensics evidence in court

Computer Forensics

- To produce evidence for digital cases
- Evidence admissible in court is reproducible and verifiable
- Verifiable though chain of custody

Types of Computer Forensics

There are primarily two types of investigation: Public and Private/Corporate

Public/Criminal investigation

- Context criminal case
- Conducted by law enforcement
- Driven by statues of criminal law

Forensics types

- Desktop Forensics
- Network Forensics
- Mobile Forensics
- Database Forensics

Example of Criminal Cases

- Money Laundering Theft
- Pedophilia
- Drug peddling
- Attacks with intend to denied services etc.

Private/Civil Investigation

- Occurs in civil cases
- Conducted by corporation
- Expensive hence civil suits turns internal affair in corporate environment
- Using policies to address problems
- Driven by statues of the civil law

Challenges in Digital Forensics

- Anti Forensics tools
- Complexity of digital devices and systems
- Volume of data to be analyzed
- Privacy and legal issues related to data collection and use.

End of Lecture